Tampereen yliopisto

Kai Lehdikkö

YKSITYISYYDEN KATOAMISEN UHKA TIETOYHTEISKUNNASSA

Informaatioteknologian ja viestinnän tiedekunta
Kandidaatintutkielma
Joulukuu 2019

TIIVISTELMÄ

Kai Lehdikkö: Yksityisyyden katoamisen uhka tietoyhteiskunnassa
Kandidaattitutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Joulukuu 2019

Tässä kirjallisuuskatsauksessa tarkastellaan muutoksia ihmisten käsityksissä yksityisyydestä sekä verkkoturvallisuudesta internetin yleistymisen myötä. Käsitellään millaisia käsityksiä yksityisyydestä ilmenee yhteiskunnan digitalisoitumisen myötä sekä mitä tehdään yksityisyyden säilyttämiseksi aikana, jona tietoa kerätään enemmän kuin koskaan aiemmin. Tarkastellaan myös yksilöiden toimintaa yksityisyyden turvaamiseksi ja onko tämä toiminta ristiriidassa tutkimuksista saatujen tietojen kanssa.

Tutkielmassa käsiteltyjen artikkelien perusteella havaittiin nuorempien ihmisten keskuudessa korkeampaa taitotasoa kuin vanhemmilla ihmisillä verkon yksityisyysasioissa, yhdistettynä vähäisempään murehtimiseen yksityisyyttä uhkaaviin tekijöihin. Yksityisyyttä uhkaavat tekijät tiedostettiin, mutta verkon sosiaalisessa kanssakäymisessä ilmeneviä uhkia aliarvioitiin, kun taas ohjelmistopohjaiset uhat otettiin vakavasti. Vastauksena inhimillisen tekijän luomiin tietosuojariskeihin esitellään sosiaalisen median alustoille kehiteltyä agenttipohjaista tietosuojaa parantavaa ratkaisua sekä henkilökohtaisen datan asenteiden mittaamiseen luotua mittaria avustamaan IT-alan ammattilaisia.

Avainsanat: Tietosuoja, Tietoturvallisuus, Yksityisyys

1 Johdanto

Muutokset yhteiskunnassa ovat aiheuttaneet todennäköisesti pysyviä muutoksia siinä, mitä tarkoitamme yksityisyydellä. Warren ja Brandeis (1890) määrittelivät artikkelissaan yksityisyyden oikeutena tulla jätetyksi rauhaan (“The right to be left alone”). Digitalisaation myötä nykyisessä tietoyhteiskunnassa yksityisyydellä on jo varsin erilainen sekä monisyisempi merkitys eikä yksiselitteistä määritelmää yksityisyydelle olekaan; yksityisyys voidaan nähdä kontekstiriippuvaisena ilmiönä (Martin 2012).

Keskustelu yksityisyydestä keskittyy nykyään usein muun muassa kerättyjen henkilötietojen hallintaan ja siihen miten näitä tietoja keräävät tahot niitä käyttävät. Tämä on nähtävissä esimerkiksi Euroopan Unionin vuonna 2018 asettamassa yleisessä tietosuoja-asetuksessa (GDPR), joka keskittyy nimenomaan henkilötietojen käsittelyn sääntelyyn. Sen sijaan että kansalaiset vaatisivat saada tulla jätetyksi rauhaan, koetaan aidon yksityisyyden tavoittelemisen sijaan tärkeämmäksi se, että kun dataa kerran kerätään, tulee sitä keräävien tahojen käsitellä sitä niin, ettei siitä koidu haittaa kansalaisille. Pyrin selvittämään, kuinka hyvin edellä mainittu väite kuvastaa ihmisten asenteita yksityisyyteen ja mikä olisi tarpeen, jotta yksityisyytemme pysyisi turvattuna.

Tutkielman lähteet on haettu Tampereen yliopiston sähköisistä aineistoista (Andor) sekä IEEE- ja ACM-tietokannoista. Lähteet valittiin vertaisarvioiduista tieteellisistä artikkeleista, jotka oli julkaistu kahdeksan vuoden sisään (2012-2019). Lähteitä rajattiin niin, ettei sosiaalisen median tietoturvaa käsittelevät artikkelit päässeet valta-asemaan tutkielman lähteissä, koska tarkoituksena on tarkastella yksityisyyttä yleisesti ilman, että suositummat alustat painottuvat tutkielmassa liiaksi. Koska sosiaalinen media kuitenkin on merkittävä tekijä tietoyhteiskunnan yksityisyysaiheisessa keskustelussa, on tutkielmaan otettu lähteiksi mukaan myös sosiaalisen median tutkimuksia. Tutkielmassa käsiteltävissä artikkeleissa oli muutama relevantti lähdemateriaaliksi sopiva vanhempi julkaisu, jotka poikkeuksellisesti otettiin osaksi tutkielman lähdemateriaalia iästään huolimatta. Nämä artikkelit koskivat termimäärittelyä sanalle ”yksityisyys”, joka pohjautuu Warrenin ja Brandeisin artikkeliin vuodelta 1890, sekä tutkielmassa keskeisessä asemassa olevaa käsitettä yksityisyysparadoksi (privacy paradox). Yksityisyysparadoksiksi kutsutaan ilmiötä, jossa käyttäjät väittävät pyrkivänsä turvaamaan yksityisyytensä, mutta käytännössä ovat hyvinkin valmiita jakamaan yksityistietojaan niitä pyytäville tahoille (Norberg ja muut 2007).

Tutkielmassa esiintyviin keskeisiin käsitteisiin lukeutuvat etenkin *tietoturvallisuus* ja *tietosuoja*. Niillä englanninkielisillä IT-alan termeillä joilla ei ole vakiintunutta suomenkielistä vastinetta, käytetään joko suoraa suomennusta tai sopivaa keksittyä termiä. Tietoturvallisuudesta puhuttaessa tarkoitetaan tiedon saatavuuden,

luottamuksellisuuden ja eheyden turvaamista (kyberturvallisuuskeskus 2019). Tietosuoja puolestaan käsittelee henkilöitä yksilöivien tietojen turvaamista (tietosuojavaltuutetun toimisto 2019a). Yksityisyyteen liittyvät lailliset säädökset kuten yleinen tietosuoja-asetus lasketaan myös osaksi tietosuojaa.

Tutkielmassa käydään läpi ensin luvussa 2 sitä, miten yksityisyyttä verkossa on tutkittu ja miten yksityisyys ilmenee kuluttajien näkökulmasta. Luvussa 3 tuodaan esille esimerkkejä siitä miten yksityisyyttä ja tietoturvaa ollaan pyritty kohentamaan IT-alan ammattilaisten toimesta. Tämän jälkeen luvussa 4 havainnollistetaan miten ongelmallista yksityisyyden suojeleminen nykyään on, osittain siitä syystä että tavallisen käyttäjän sanat ja teot tietoturvan ja yksityisyyden merkityksestä ovat usein ristiriidassa keskenään. Tämän jälkeen luvussa 5 on pohdintaa siitä mitä tutkielmassa on saatu selville. Lopuksi luvussa 6 on yhteenvetona tutkielmassa läpi käydyistä artikkeleista tehtävät johtopäätökset ja tulkinta siitä mitä näistä johtopäätöksistä voidaan päätellä yksityisyyden asemasta tietoyhteiskunnassa.

2 Miten yksityisyyttä verkossa on tutkittu

Tässä luvussa tarkastellaan tutkimuksia, joissa tutkimusaiheena on ollut yksityisyys ja sen merkitys kunkin tutkimuksen käyttäjäryhmälle. Käsitellään ensin millaisia eroja kulttuurilliset ja sukupolvelliset tekijät saavat aikaan kuluttajien näkemyksissä yksityisyyteen. Tämän jälkeen tarkastellaan miten yleinen tietosuoja-asetus (GDPR) on otettu kuluttajien keskuudessa vastaan. Lopuksi paneudutaan kuluttajien asenteisiin yksityisyyden turvaamisessa ja siihen millaisina kuluttajat näkevät verkon eri tietoturvauhat.

2.1 Kulttuurilliset ja sukupolvelliset tekijät

Keskusteltaessa yksityisyyden merkityksestä voidaan huomata eri sukupolvilla olevan poikkeavat näkemykset siitä, kuinka merkitsevää yksityisyyden varjeleminen internetissä on. Tämän lisäksi myös oman yksityisyyden turvaamisen taitotaso voi vaihdella sukupolvittain. Miltgen ja Peyrat-Guillard (2014) suorittivat aihetta tutkiakseen laadullisen tutkimuksen, jossa selvitettiin Euroopan kansalaisten yksityisyyteen liittyviä huolenaiheita, ottaen huomioon ikäluokat sekä kulttuurilliset tekijät. Tutkimuksessa suoritettiin jaottelu nuoriin (15-24-vuotiaat) ja aikuisiin (25-70-vuotiaat). Tämän lisäksi kulttuurilliset erot tuotiin esille tekemällä myös maantieteellinen jaottelu pohjois-, itä-, länsi- ja eteläeurooppalaisiin ryhmiin. Tutkimuksen hypoteesit olivat:

1. Eri Euroopan maista kotoisin olevat ihmiset poikkeavat siinä mitä pitävät yksityisyyteen liittyvinä huolenaiheina ja miten he pyrkivät toimimaan yksityisyytensä turvaamiseksi. Erityisesti kollektiivisista kulttuureista peräisin olevat ihmiset ovat luottavaisempia tietojensa käsittelyn suhteen sekä

avoimempia jakamaan yksityiseksi nähtäviä tietoja verrattuna individualistisempiin kulttuureihin.

2. Eri ikäryhmät poikkeavat toisistaan siinä mitä pitävät yksityisyyteen liittyvinä huolenaiheina ja miten he pyrkivät toimimaan yksityisyytensä turvaamiseksi. Nuorilla ihmisillä on positiivisemmat näkemykset yksityisyyteen liittyvissä huolenaiheissa kuin vanhemmilla ihmisillä.

Kulttuurin vaikutus yksityisyyteen ilmeni tutkimuksessa siten, että pohjois- ja eteläeurooppalaisilla havaittiin näkemyseroja vastuunjaon ja luottamuksen välillä. Tämän lisäksi etelä- ja itäeurooppalaiset olivat eri mieltä kontrollin ja vapaaehtoisuuden suhteen. Eteläeurooppalaiset kokivat että heillä on mahdollisuus valita mitä tietoja ja kuinka paljon jakavat, siinä missä itäeurooppalaiset kokivat että tietoja on periaatteessa pakko jakaa (Miltgen ja Peyrat-Guillard 2014).

Tälle katsaukselle olennaisimmat löydökset tutkimuksessa ilmenivät ikäluokkia tutkittaessa käänteisen yksityisyysparadoksin ilmenemisenä tutkimustuloksissa. Tutkimuksessa havaittu käänteinen yksityisyysparadoksi osoitti, että vähäisempi yksityisyysasioiden murehtiminen, jota esiintyi enemmän nuorissa kuin aikuisissa, yhdistyi kuitenkin nuorilla aikuisia taitavampaan yksityisyyden turvaamiseen. Nuorten lähestymistapa yksityisyyteen on kuvailtavissa erilaisena verrattuna vanhempiin ihmisiin siten, että nuoret ovat erityisen taitavia kontrolloimaan sitä ketkä heistä kerättyä dataa hallinnoivat (Miltgen ja Peyrat-Guillard 2014).

Regan ja muut (2013) käsittelivät sukupolvien välisiä näkemyseroja yksityisyyden suhteen tutkimuksessaan jossa analysoidaan 30 vuoden ajalta tehtyjä kyselytutkimuksia, pyrkimyksenä havaita millaisia nämä oletetut näkemyserot ovat. Tutkimuksessa analysoitiin vastauksia vuosilta 1974, 1983 ja 1993 liittyen salakuunteluun (engl. wiretapping) sekä valtion keräämän datan kokemisesta uhkana yksityisyydelle vuosilta 1985, 1996 ja 2006. Analysoidut vastaukset jaoteltiin sukupolvittain. Näiden sukupolvien vuosimääritelmät ja nimeämisperinteet vaihtelevat ja täten artikkelin käyttämät nimet ja vuosiluvut poikkeavat jonkin verran suomalaisista vastineistaan. Tässä käytetään suomalaisia nimiä tai suoraa käännöstä yhdessä artikkelin vuosilukujen kanssa. Jaottelu oli seuraavanlainen (Regan ja muut 2013):

1. Suurin sukupolvi (The Greatest Generation) kattaa ennen 1928 syntyneet
2. Veteraanit (The Silent Generation) kattaa 1928-1945 syntyneet
3. Suuret ikäluokat (Baby Boomers) kattaa 1946-1964 syntyneet
4. X-sukupolvi (Generation X) kattaa 1965-1980 syntyneet
5. Milleniaalit (Millennials) kattaa 1980 jälkeen syntyneet

Tutkimuksen hypoteesina oletettiin sukupolvien välillä olevan eroavaisuuksia näkemyksissä yksityisyyteen. Tämä oletus pohjautui aiemmin tehtyihin tutkimuksiin aiheesta. Suurimman sukupolven ja veteraanien edustajien oletettiin olevan sukupolvista

luottavaisimpia valtioon. Suurten ikäluokkien edustajien oletettiin olevan eniten huolissaan yksityisyydestä, kun milleniaalien puolestaan oletettiin olevan vähiten huolissaan yksityisyydestä. X-sukupolven oletettiin yhtyvän näkemyksissään enemmän suuria ikäluokkia edeltäviin sukupolviin. Oletuksena oli myös, että jokaisen sukupolven kiinnostus yksityisyyden turvaamiseen kasvaisi nuoruusvuosista saavuttaen huippunsa keski-iässä ja laskisi jälleen iän karttuessa. Lopuksi, nuorempien sukupolvien edustajat jotka ovat kasvaneet teknologian parissa, oletettiin olevan luottavaisempia teknologiaan ja murehtivan yksityisyydestään vähemmän kuin vanhemmat sukupolvet, riippumatta muista elämäntavoista.

Regan ja muut (2013) raportoivat että salakuuntelun suhteen kaikki sukupolvet muuttuivat myötämielisemmiksi sitä kohtaan ajan kuluessa. Suuret ikäluokat olivat vahvemmin salakuuntelua vastaan, mutta kaikki sukupolvet olivat kuitenkin suurimmilta osin salakuuntelua vastaan ja kokivat sen uhkana yksityisyydelle. On kuitenkin aiheellista huomioida, että milleniaaleilta ei tätä analyysiä suoritettu sukupolven nuoruuden takia. Valtion datankeruun suhteen analyysi ei tuottanut selkeää jakoa sukupolvittain. Selville saatiin vain, että datan keruu koettiin uhkana yksityisyydelle vahvimmin kaikkien sukupolvien osalta vuonna 1996 ja vuoteen 2006 mennessä tämä uhan kokemus laski huomattavasti jokaisella sukupolvella. Milleniaaleilta analysoitavaa dataa oli kuitenkin vain vuodelta 2006.

Tässä osassa käsiteltyjen tutkimusten avulla voidaan huomata nuorempien sukupolvien, etenkin milleniaalien, välittävän vähemmän yksityisyydestään kuin vanhempien sukupolvien, mutta samalla he hallitsevat vanhempia sukupolvia paremmin oman yksityisyytensä turvaamisen koska ovat varttuneet tietotekniikan parissa. Tämä saattaa olla osasyynä siihen, että nuoremmat sukupolvet eivät näe yksityisyyttä enää absoluuttisena itseisarvona jonka toteutumista tulee tavoitella, vaan eräänlaisena valuuttana jolla tehdä kauppaa.

2.2 Yleisen tietoturva-asetuksen vastaanotto

Euroopan Unionin asettama yleinen tietosuoja-asetus (GDPR) nosti pinnalle keskustelua kuluttajien henkilötietojen käsittelystä. Yleinen tietosuoja-asetus korvasi vuonna 2018 aiemmin voimassa olleen tietosuojadirektiivin, joka oli lainsäätäjille suunnattu toimintaohje, siinä missä yleinen tietosuoja-asetus on henkilötietojen käsittelyä sääntelevä laki (Tietosuojavaltuutetun toimisto 2019b). Yleisen tietosuoja-asetuksen tarkoituksena on sekä yhtenäistää EU-maiden tietosuojasääntelyä että parantaa kansalaisten henkilötietojen suojaa, sillä vanha tietosuojadirektiivi vuodelta 1995 ei pysynyt digitaalisen kehityksen mukana, vaan jäi auttamatta jälkeen sekä määrittelyn että valvomisen osalta.

Presthus ja Sørum (2018) tutkivat kyselytutkimuksen avulla millaisia ajatuksia ja odotuksia tämä uudistus tietosuojalaissa herätti norjalaisissa kuluttajissa. Kyselytutkimus

sisälsi Likert-asteikollisia kysymyksiä, monivalintakysymyksiä sekä avoimia kysymyksiä joihin koehenkilöt saivat vastata omin sanoin. Tutkimuksen otoskoko oli 216. Kysymykset laadittiin täysin yleisen tietosuoja-asetuksen käsittelemien asioiden pohjalta ja sidottiin kuluttajille arkipäivisiin konteksteihin kuten sosiaalisen median käyttöön ja omien henkilötietojen luovuttamiseen erilaisia etuja tai alennuksia vastaan. Presthusin ja Sørumin (2018) tutkimuksesta selvisi, että tietoisuus yleisestä tietosuoja-asetuksesta vaihteli jonkin verran. Noin 47 % vastaajista tiesi mikä yleinen tietosuoja-asetus on ja noin 27 % vastaajista kertoivat etteivät tienneet tarkalleen ottaen mikä yleinen tietosuoja-asetus on, vaikka olivat siitä kuulleet. Loput vastaajat joko olivat vain kuulleet yleisestä tietosuoja-asetuksesta tietämättä mihin se liittyy tai eivät olleet koskaan kuulleetkaan siitä. Tämän lisäksi tutkimus osoitti, että kuluttajat olivat huolissaan yksityisyyden puolesta joko vahvasti (34 %) tai jonkin verran (55 %). Loput 11 % jakautuivat vähäisesti huolestuneiden ja välinpitämättömien välille. Vaikka yleinen tietosuoja-asetus siis tunnistettiin melko hyvin ja yksityisyys koettiin pääasiassa tärkeäksi, osoittivat kyselyyn vastanneet skeptisyyttä asetuksen kykyyn turvata kuluttajien yksityisyys, koska usko yritysten haluun tai kykyyn noudattaa asetusta oli vähäinen. Osa vastaajista pelkäsi, että suuret yritykset keksivät keinoja välttää yleisen tietosuoja-asetuksen rikkomisesta seuraavat sanktiot ja näin ollen asetus jäisi lähinnä pienempien yritysten murheeksi eikä kuluttajien yksityisyys olisi sen turvatumpi kuin tähänkään mennessä.

Yksityisyyden merkitys nousi esille Presthusin ja Sørumin (2018) raportoidessa kyselyyn vastanneiden kertovan luottamuksensa suurten yritysten kuten Facebookin halukkuuteen turvata käyttäjiensä yksityisyys olevan vähäistä ja täten monet vastaajat (69 %) toivoivat, että yleisellä tietosuoja-asetuksella olisi positiivisia vaikutuksia sosiaalisen median yritysten toimintaan yksityisyydensuojan saralla. Myös vastaajien valmius luovuttaa omia tietojaan erilaisia etuja vastaan jäi lähinnä nimitietojen ja sähköpostin tasolle, vaikkakin pieni osa vastaajista oli valmiina luovuttamaan hyvinkin herkkäluontoisia tietoja kuten IP-osoite tai henkilötunnus. Yleisesti ottaen yksityisyyttä ei koettu kyselyssä suinkaan merkityksettömäksi ja yleinen tietosuoja-asetus otettiin vastaan positiivisena muutoksena tietosuojalaissa, etenkin niiden kuluttajien osalta jotka olivat jo ennestään paneutuneet verkon yksityisyyttä ja tietoturvaa koskeviin ongelmiin (Presthus ja Sørum (2018).

2.3 Verkossa toimimisen riskit yksityisyydelle

Verkossa toimiminen alustasta riippumatta sisältää aina tietoturva- ja yksityisyysriskejä. Schaik ja muut (2017) tutkivat Iso-Britannian ja Amerikan Yhdysvaltojen yliopisto-opiskelijoiden riskienhallintataitoja verkossa sekä millaisina yliopisto-opiskelijat havaitsevat verkon eri tietoturvariskit. Nuorilla havaittu vähäinen murehtiminen yksityisyyden vaarantumisesta ilmeni jo Miltgenin ja Peyrat-Guillardin

(2014) tutkimuksessa ja täten onkin aiheellista selvittää miten erilaiset tietoturvariskit arvotetaan ja mitä on tehtävissä jotta asenteet muuttuisivat niin ettei yksilöiden saati yritysten tietoturva tule kärsimään siitä, että kaikkia verkon tietoturvariskejä ei oteta kyllin vakavasti. Schaik ja muut (2017) asettivat tutkimuksessaan neljä tutkimuskysymystä liittyen verkossa toimimisen tietoturvariskeihin:

1. Millaisina yliopisto-opiskelijat havaitsevat verkon eri tietoturvariskit?
2. Miten yliopisto-opiskelijat suojautuvat verkon eri tietoturvariskeiltä?
3. Mitkä ovat yliopisto-opiskelijoiden verkon eri tietoturvariskien arvottamista selittävät tekijät?
4. Mitkä tekijät selittävät yliopisto-opiskelijoiden varautumista verkon eri tietoturvariskeihin?

Verkon tietoturvariskit jaoteltiin kuuteentoista eri riskiin jotka jaoteltiin neljään eri kategoriaan (identiteetti, monitorointi, online-sosiaalinen ja ohjelmisto). Riskit olivat identiteettivarkaus, tietojenkalastelu, verkkoseuranta, verkkoahdistelu, verkkokiusaaminen, käyttäjän manipulointi, valeidentiteetillä huijaaminen, virukset, vakoiluohjelmat, Troijan hevoset, näppäilytallentimet, bottiverkot, evästeet, huijariohjelmat (rogueware), nollapäivähaavoittuvuudet ja sähköpostiosoitteiden kerääminen. Näille riskeille oli myös kaksi vertailumuuttujaa: tiedonhaku verkosta ja tiedonjako sosiaalisessa mediassa. Riskeille laskettiin keskiarvot ja luottamusvälit. Korkeampi keskiarvo viittasi siihen, että riski arvotettiin vakavammaksi. Vakavimpana riskinä koettiin identiteettivarkaus (k.a. 5,94) ja pienimmäksi riskiksi koettiin evästeet (k.a. 3.39). Vertailumuuttujana toiminut tiedonhaku verkosta koettiin kaiken kaikkiaan vähiten riskialttiiksi toiminnaksi (k.a. 2,87) ja tiedonjako sosiaalisessa mediassa koettiin vain jonkin verran evästeitä riskialttiimmaksi (k.a. 4,61) (Schaik ja muut 2017).

Schaik ja muut (2017) havaitsivat yliopisto-opiskelijoiden käyttävän virustorjuntaohjelmia ja päivittävän käyttämiään sovelluksia niin, että ne pysyvät ajan tasalla, mutta vakoiluohjelmien tai palomuurien käyttö oli vähäisempää. Valtaosa ennaltaehkäisevästä toiminnasta myös koski ainoastaan ohjelmistopuolen riskeiltä suojautumista, jättäen käyttäjät mahdollisesti alttiiksi muille riskityypeille kuten tietojenkalastelulle ja verkkoahdistelulle. Tätä ilmiötä selittää se, että tietoturvariskejä arvotettiin yliopisto-opiskelijoiden toimesta suuremmiksi silloin, kun niiden seuraukset ilmenevät välittömästi. Virukset ja muut ohjelmistopuolen tietoturvariskit ovat välitön uhka jonka seuraukset voivat ilmetä hyvin nopeasti käyttäjälle, kun taas online-sosiaaliset uhat realisoituvat hitaammin, jos ollenkaan. Myös uhan seurausten vakavuus selitti miten suureksi kyseisen tyyppisiä tietoturvariskejä arvotettiin. Tämä selittää osittain miksi identiteettivarkauden sijoittumisen tietoturvariskien listalta korkeimmalle; sen seuraukset koetaan varmasti hyvin vakaviksi. Schaik ja muut (2017) huomasivat, että parempaa varautumista verkon tietoturvariskeiltä ennusti käyttäjän kokemus siitä, että hallitsee

tietokoneiden käytön. Ne yliopisto-opiskelijat jotka kokivat hallitsevansa tietokoneensa tietoturva-asiat käyttivät muun muassa aktiivisemmin virustorjuntaohjelmia.

Tässä kohdassa käsitellyn Schaikin ja muiden (2017) tutkimuksen pohjalta voidaan tarkentaa tähän mennessä havaittua lievää välinpitämättömyyttä yksityisyyden riskejä kohtaan nuorten käyttäjien keskuudessa sen verran, että vähäinen murehtiminen yksityisyyden puolesta korostuu eniten online-sosiaalisten riskien merkityksen aliarvioinnissa, kun taas ohjelmistopohjaiset uhat otetaan vakavasti. Tämä asettaa kuluttajat asemaan jossa riskinä verkossa eivät enää välttämättä olekaan vaikkapa tietomurrot, vaan toiset käyttäjät jotka eivät tule ajatelleeksi mitä sisältöä jakavat verkossa. Mielenkiintoisena tuloksena ilmeni myös se, että vaikka suurin osa suurimmiksi arvioiduista riskeistä kuuluivat kategoriaan online-sosiaalinen, ei tiedonjakoa sosiaalisessa mediassa kuitenkaan mielletty riskialttiiksi toiminnaksi yliopisto-opiskelijoiden keskuudessa.

2.4 Päätelmiä

Tässä luvussa käsitellyistä tutkimuksista olennaisimpina seikkoina voidaan tuoda esille nuorten ihmisten parissa havaittu korkeampi luottamus omiin tietoteknisiin taitohin yhdistettynä pienempään yksityisyyden uhkien murehtimiseen, joka johti havaittuun käänteiseen yksityisyysparadoksiin (Miltgen ja Peyrat-Guillard 2014). Nuorten ihmisten parissa ilmenee kuitenkin taipumusta vähätellä verkossa toimimisen mahdollisia sosiaalisia yksityisyyttä uhkaavia tekijöitä verrattuna ohjelmistopuolen riskeihin (Schaik ja muut 2017). Presthusin ja Sørumin (2018) tutkimus yleisestä tietosuoja-asetuksesta antoi kuitenkin viitteitä siihen, että sosiaalisen median alustojen toimintaa yksityistietojen keruun suhteen halutaan tarkemman kontrollin alle. Nämä tulokset viittaavat jo jonkin verran yksityisyysparadoksiksi kutsutun ilmiön olemassaoloon; on puhetta yksityisyyden turvaamisen puolesta, mutta toiminta ja havaitut asenteet kertovat muuta.

3 IT-alan ammattilaiset ja yksityisyyden turvaaminen

Koska verkossa toimiminen, etenkin sosiaalisen median alustoilla, edellyttää yksityisyyden turvaamiseksi panostamista sekä käyttäjiltä että palveluntarjoajilta, tuodaan tässä luvussa esille kaksi artikkelia joista ilmenee miten IT-alan ammattilaiset työskentelevät yksityisyyden turvaamisen puolesta ja miten käyttäjien asenteet ja toiminta ovat välittömässä yhteydessä toisten käyttäjien yksityisyyteen. Tähän mennessä on ilmennyt, että etenkin nuoret aikuiset asennoituvat huomattavasti kevyemmin niihin riskeihin joita ilmenee verkon sosiaalisissa konteksteissa, kuin ohjelmistopuolen tietoturvauhkiin (Schaik ja muut 2017). Tästä syystä IT-alan ammattilaisten on täytynyt tutkia käyttäjien välistä tiedon jakamista muun muassa sosiaalisen median alustoilla ja pyrkiä löytämään ne tekijät, jotka voivat toimia riskitekijöinä käyttäjien yksityisyydelle.

Ongelmallista tässä on kuitenkin se, että eri käyttäjillä saattaa olla hyvinkin erilaiset käsitykset siitä mitä tietoa toisista käyttäjistä voi jakaa ilman erillistä lupaa ja millaisen tiedon jakaminen puolestaan edellyttäisi erillistä luvan kysymistä etukäteen asianomaisilta käyttäjiltä (Kökciyan ja muut 2017). Ongelmaa ei myöskään helpota se, että todennäköisyys yksityisyyden turvaamisen sivuuttamiseen kasvaa mikäli käyttäjät kokevat sen liian työlääksi. Esimerkiksi palveluiden käyttöehtojen läpikäyminen koetaan usein työlääksi prosessiksi ja täten monet käyttäjät hyväksyvät käyttöehdot lukematta niitä läpi (Presthus ja Sørum 2018). Sosiaalisen median alustoilla käyttäjillä saattaa olla ystäviensä tai tuttaviensa kanssa sovitut yhteiset pelisäännöt siitä mitä voidaan jakaa kysymättä erikseen asiasta toisilta, mutta luultavasti tämänlainen huomaavaisuus ei ulotu tuntemattomiin käyttäjiin. Kökciyan ja muut (2017) esittelevät artikkelissaan agenttipohjaisen ratkaisun joka ei vaatisi sosiaalisen median palveluiden käyttäjiltä suurta vaivannäköä, mutta parantaisi käyttäjien yksityisyyden turvaa sekä vähentäisi niitä mahdollisia konflikteja joita voisi seurata käyttäjien näkemyseroista yksityisyysasioissa. Agenteilla tarkoitetaan ohjelmistoja jotka kykenevät havainnoimaan, päättelemään, toimimaan ja kommunikoimaan tarpeen vaatiessa muiden agenttien kanssa. Agenttien ansiosta käyttäjien ei tarvitsisi sopia keskenään mitä sisältöä toisistaan voivat jakaa, vaan vuoropuhelu tiedon jakamisesta tapahtuisi taustalla toimivien agenttien toimesta käyttäjien asettamien yksityisyysasetusten mukaisesti ja päätös sisällön jakamisesta määräytyisi tämän vuoropuhelun pohjalta ennen kuin tietoa jaettaisiin.

Kökciyan ja muut (2017) havainnollistavat sosiaalisen median käyttäjien toimintaa viidellä skenaariolla joissa kuvitteelliset sosiaalisen median alustan käyttäjät Alice ja Bob keskustelevat kuvan jakamisesta kyseisellä alustalla. Alice haluaisi jakaa alustalla kuvan jossa esiintyy Bob kädessään Oktoberfest-teemainen rannekoru. Skenaariot ovat seuraavat:

1. Alice haluaa jakaa kuvan kysymättä Bobilta.
2. Alice haluaa jakaa kuvan, mutta kysyy ensin Bobilta käykö tämä. Bob kieltää jakamasta kuvaa koska rannekoru osoittaisi Bobin osallistuneen Oktoberfest-festivaaliin.
3. Jatkona skenaarioon 2: Alice kertoo Bobille että kyseisiä rannekoruja on saatavilla myös Gifty-nimisestä liikkeestä eikä rannekoru täten välttämättä viittaa Bobin ottaneen osaa festivaaliin.
4. Jatkona skenaarioon 3: Bob yrittää tarkastaa onko Gifty auki, uskoo ettei liikkeen verkkosivuille pääse ja päättelee että kyseinen liike on lakkauttanut toimintansa.
5. Jatkona skenaarioon 4: Alice tietää että Giftyllä on toinen verkkosivu joka toimii.

Ensimmäinen skenaario kuvaa tämänhetkistä toimintaa sosiaalisessa mediassa. Tietoa jaetaan (mahdollisesti) kysymättä asianomaisilta ensin. Toinen skenaario kuvastaa vuoropuhelun alkua tiedon jakamisesta ja sisältää syyn tiedon jakamisen kieltämiselle. Kolmannessa skenaariossa lähtee käyntiin vuoropuhelu jossa käyttäjät argumentoivat tiedon jakamisen puolesta ja vastaan. Ongelmana tässä käyttäjien välisessä vuoropuhelussa on se, että skenaariosta yksi päädytään tilanteeseen jossa tietoa jaetaan mahdollisesti loukaten käyttäjän yksityisyyttä, eikä tiedon poisto verkosta jälkikäteen joissain tapauksissa tyydyttävä ratkaisu. On mahdollista että tieto on tallennettu kolmannen osapuolen toimesta toisaalle tai jaetun tiedon mahdollisesti aiheuttama vahinko on jo tapahtunut, eikä tiedon poistaminen verkosta enää auta. Myös ensimmäistä skenaariota seuraavien skenaarioiden riskinä on, että Alice päättää julkaista kuvan Bobin vastalauseista huolimatta, koska kokee etteivät Bobin perustelut kuvan jakamisen kieltämiselle ole pätevät. Tässä esille tuodun kaltaisen vuoropuhelun käyminen aina tietoa jakaessa ei luultavasti onnistuisi käyttäjiltä monista käytännön syistä, ilmeisimpänä ehkäpä vaadittujen vuoropuheluiden kasvava määrä kun jaettava tieto koskee useampia käyttäjiä sekä keskustelujen vaatima aika. Täten sosiaalisen median alustoilla voitaisiin ottaa käyttöön taustalla toimivat agentit, jotka käyvät nämä vuoropuhelut keskenään ennen tiedon jakamista. Näin käyttäjien aika ei kuluisi erimielisyyksistä keskustellen eikä tietoa tulisi jaettua ilman, että jokaisen asianomaisen kanta tiedon jakamiseen tulisi otettua huomioon (Kökciyan ja muut 2017).

Vertaillakseen agenttien antamia vastauksia skenaarioihin käyttäjien näkemyksiin siitä mitä skenaarioissa tulisi tapahtua Kökciyan ja muut (2017) suorittivat kaksi kyselypohjaista koetta, haastattelu ja verkkokysely, joissa pyrittiin selvittämään mitä koehenkilöt olettivat skenaarioissa tapahtuvan. Agentit olivat päätyneet skenaarioissa seuraaviin tuloksiin:

1. Alicen agentti jakaa kuvan konsultoimatta Bobin agenttia.
2. Alicen ja Bobin agentit käyvät keskenään vuoropuhelun, jonka päätöksenä on että Alicen agentti ei jaa kuvaa.
3. Käydyn vuoropuhelun päättyessä siihen ettei Bobin agentti kykene antamaan pätevää vasta-argumenttia Alicen agentille, jakaa Alicen agentti kuvan.
4. Bobin agentin vasta-argumentti liikkeen lakkautuksesta estää Alicen agenttia jakamasta kuvaa.
5. Alicen agentin argumentti vaihtoehtoisesta verkkosivusta kumoaa Bobin agentin argumentin ja Alicen agentti jakaa kuvan.

Koehenkilöt kävivät läpi näistä skenaarioista ensimmäiset neljä. Haastatteluun osallistui 36 henkilöä ja verkkokyselyyn 68 henkilöä. Vaikka tulokset mukailivat jonkin verran agenttien antamia vastauksia, oli eroja havaittavissa agenttien vastausten ja

koehenkilöiden vastausten lisäksi haastatelluiden koehenkilöiden ja verkkokyselyyn vastanneiden välillä. Kyselyiden tulokset ovat esillä taulukossa 1.

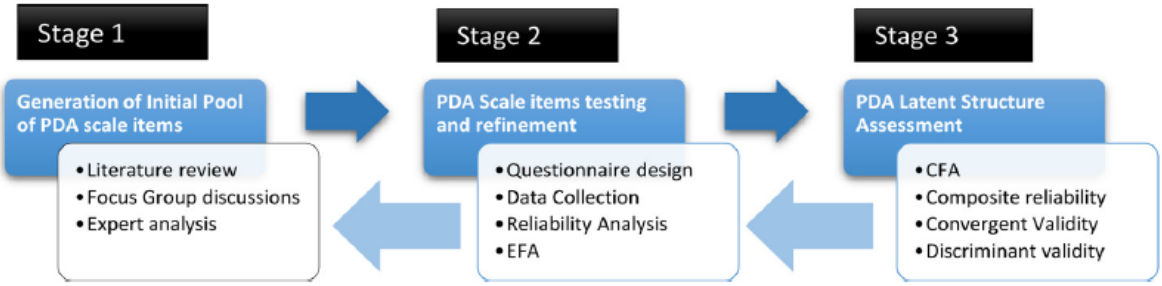
Skenaario	Haastattelu (36 henkilöä)		Verkkokysely (68 henkilöä)	
	Jakaa	Ei jaa	Jakaa	Ei jaa
1	**83,33 %**	16,66 %	**64,71 %**	35,29 %
2	5,55 %	**94,44 %**	7,35 %	**92,65 %**
3	**52,77 %**	47,22 %	20,59 %	**79,41 %**
4	2,77 %	**97,22 %**	7,35 %	**92,65 %**

Taulukko 1. Kyselytutkimuksen tulokset.

Agenttien ja haastatteluun osallistuneiden vastaukset skenaaroihin ovat samankaltaiset, vaikkakin kolmannessa skenaariossa haastatellut koehenkilöt ovat jakautuneet lähes tasan jakamisen ja jakamatta jättämisen välillä (52,77 % vs. 47,22 %). Verkkokyselyyn vastanneista sen sijaan huomattavasti suurempi osa (35,29 %) oli valmiina olemaan jakamatta kuvaa ensimmäisessä skenaariossa verrattuna haastateltuihin koehenkilöihin (16,66 %). Verkkokyselyn koehenkilöt kunnioittivat tässä tapauksessa kaiken varalta Bobin yksityisyyttä tietämättä mitään tämän yksityisyyspreferensseistä. Kolmannen skenaarion kohdalla verkkokyselyyn vastanneet ottivat selkeästi Bobin yksityisyyttä kunnioittavan kannan, perustellen tätä siten ettei Alicen argumentti jakamisen puolesta ollut kyllin vahva. Verkkohaastattelun koehenkilöissä ilmeni taipumusta olla mielummin jakamatta tietoa kuin riskeerata loukkaamasta toisten yksityisyyttä. Kökciyan ja muut (2017) pitivät kyselytutkimuksen tuloksia lupaavana merkkinä argumentaatiopohjaisten agenttien toimivuudesta, koska tulokset osoittivat uuden informaation aiheuttavan muutoksia koehenkilöiden päätöksissä jakaa tietoa ja tämä mukailee agenttien toimintaperiaatetta. Tämä on esillä taulukossa 1, missä näkyy haastateltujen koehenkilöiden kannan muutos jakamisen suhteen skenaarioissa esitettyjen uusien argumenttien pohjalta. Verkkokyselyn tuloksia tulkitessa skenaarion kolme kohdalla nähdään, että agentit voivat myös päätyä hyvin erilaisiin lopputuloksiin kuin koehenkilöt. Verkkokyselyn koehenkilöt perustelivat puoltaessaan Bobin yksityisyyttä skenaariossa kolme sillä, että Alicen argumentti ei ollut kyllin vahva oikeuttaakseen Bobin yksityisyyden loukkaamisen jakamalla kuvan. Tämä argumenttien painoarvojen arviointi ei kuitenkaan ollut vielä osana Kökciyanin ja muiden (2017) agentteja, mutta sen sisällyttäminen agenttien algoritmeihin olisi kyllä mahdollista.

Kökciyanin ja muiden (2017) tutkimus osoitti hyvin, kuinka käyttäjien asenteet yksityisyyden piiriin kuuluvien tietojen suhteen voivat jakautua samoissa tilanteissa hyvinkin vahvasti ja täten IT-alan ammattilaisten tulee paneutua myös käyttäjien asenteiden tutkimiseen. Seuraavaksi esitellään lyhyesti PDA-mittaria (Personal Data Attitude-measurement instrument), jonka tarkoituksena on auttaa IT-alan ammattilaisia selvittämään verkon käyttäjien asenteita henkilökohtaisen datan keruun suhteen. Tällä

hetkellä tietoa käyttäjien asenteista ei ole tarpeeksi siihen, että yksityisyyteen liittyviin ongelmiin voitaisiin varautua kyllin tehokkaasti uusia palveluita kehiteltäessä (Addae ja muut 2017). PDA-mittarin kehittämisen työvaiheet esitetään kuvassa 1.



Kuva 1. PDA-mittarin kehittämisen työnkulku (Addae ja muut 2017)

Mittarin kehittäminen aloitettiin kuvan 1 mukaisesti vaiheesta yksi käymällä läpi aiempaa tutkimustietoa kirjallisuuskatsauksena, josta kerätty tieto uudelleenmuotoiltiin reflektoimaan neljää eri henkilökohtaista datatyyppiä: e-mail ja sosiaalinen media (henkilökohtainen online-data); taloudellinen ja terveys ((verkosta) poiskytketyt tiedot). Tämän jälkeen jouduttiin tekemään eksploratiivinen tutkimus, koska valmista mitta-asteikkoa asenteille henkilökohtaista dataa kohtaan ei löytynyt. Kirjallisuuskatsauksen kautta saatu tieto myös varmennettiin järjestämällä kohderyhmähaastattelu, jossa avointen kysymysten avulla jaoteltiin yksilöiden näkemyksiä edellämainittuihin henkilökohtaisiin datatyyppeihin. Tämä johti sadan PDA:ta kuvaavan tekijän löytymiseen, mutta näistä 64 eliminoitiin koska ne olivat liian spesifejä. Vaiheessa kaksi jäljelle jääneet 46 PDA:ta kuvaavaa tekijää tiivistettiin edelleen 34:ksi PDA:ta kuvaavaksi toteamukseksi. Näiden toteamusten avulla suoritettiin verkkokysely, jossa vastaajat vastasivat satunnaistettuihin toteamuksiin Likert-asteikon tyyppisen asteikon avulla. Kyselyn lopullinen otoskoko oli 247 ja vastaajien ikä vaihteli 17-67 vuoden välillä iän keskiarvon ollessa 36 vuotta. Vaiheessa kaksi suoritettiin myös toteamusten reliabiliteetin testaus ja eksploratiivinen faktorianalyysi (EFA). Reliabiliteetin testauksen tulokset viittasivat korkeaan reliabiliteettiin ja faktorianalyysin tuloksena saatiin lopulta kuusi faktoria, jotka selittivät 63,983 % 31:n PDA:ta kuvaavan toteamuksen varianssista. Nämä faktorit nimettiin seuraavasti (Addae ja muut 2017):

1. Suojaava käytös (Protective behaviour/interest)
2. Yksityisyyshuolet (Privacy/confidentiality concerns)
3. Hinta-hyöty (Cost-benefit)
4. Tiedostus (Awareness)
5. Vastuullisuus (Responsibility)
6. Turvallisuus (Security)

Vaiheessa kolme suoritettiin konfirmatorinen faktorianalyysi joka tuki valittua kuuden faktorin jakoa. Myös komposiittireliabiliteetin, konvergentin validiteetin ja diskriminatorisen validiteetin tulokset viittasivat mittarin luotettavuuteen (Addae ja muut

2017). Löytyneiden kuuden faktorin ja neljän aiemmin mainitun henkilökohtaisen datatyypin välillä suoritettiin vertailu, jossa faktorit asetettiin riippuviksi muuttujiksi ja datatyypit riippumattomiksi muuttujiksi. Testeistä ilmeni, että henkilökohtaisen datan tyyppi ennusti tilastollisesti merkitsevästi sekä suojaavan käytöksen ($p < 0,05$), että yksityisyyshuolien ($p < 0,05$) faktorien toteamuksiin annettuja vastauksia. Havaittiin myös, että suojaavaa käytöstä ilmeni eniten terveys- ja e-mail-tyyppisen datan yhteydessä (Addae ja muut 2017).

Tutkimuksessa kehitellyn mittarin ja jo olemassaolevien samantyyppisten mittareiden erona on se, että olemassaolevat mittarit eivät keskity nimenomaan yksilöiden asenteiden tutkimiseen tai siihen mitä yksilöt mieltävät henkilökohtaisen datan käsitteen kattavan. Tämän johdosta saatujen tulosten uskotaan olevan avuksi IT-alan tietoturvallisuuden tutkimuksen saralla ja myös suunnittelun käytännöissä tarjoamalla:

1. Rakenteet yksilöiden asenteiden kuvailemiseen henkilökohtaisen datan puitteissa; ja
2. mittarin joka on helposti muokattavissa ja käytettävissä mittaamaan eri konteksteissa mielenkiinnon kohteena olevia huolia tai preferenssejä mitä tulee tietoturvasuunnitteluun

PDA-mittarin kaltaisen mittarin olemassaolon myötä IT-alan ammattilaisten on helpompi luokitella käyttäjiä profiloimalla nämä tietoturvaan liittyvien asenteiden suhteen ja huomioida näiden asenteiden mahdolliset vaikutukset käyttäjien tietoturvaan palveluita kehittäessä (Addae ja muut 2017).

4 Miten käyttäjien sanat ja teot ovat ristiriidassa - Yksityisyysparadoksi

Tässä luvussa käydään läpi Norbergin ja muiden (2007) artikkelin sekä Barthin ja Jongin (2017) kirjallisuuskatsauksen avulla yksityisyysparadoksina tunnettua ilmiötä. Yksityisyysparadoksi ilmenee Norbergin ja muiden (2007) artikkelissa tehdyssä tutkimuksessa käyttäjien sanojen ja tekojen ristiriitana henkilökohtaisten tietojen jakamisessa. Yksityisyysparadoksin havainnollistamiseksi käydään ensin läpi Norbergin ja muiden (2007) tutkimuksen hypoteesit:

1. Yksilöt jakavat tosiasiassa huomattavasti enemmän tietoa itsestään kuin ilmoittavat aikovansa jakaa.
2. Riskien tiedostamisella on negatiivinen vaikutus yksilöiden ilmoittamaan aikomukseen jakaa tietoa itsestään.
3. Luottamuksella on huomattava positiivinen vaikutus yksilöiden jakaman tiedon määrään.

Näitä hypoteeseja testattiin kahdella kaksiosaisella kokeella. Ensimmäisen kokeen ensimmäisessä vaiheessa koehenkilöt vastasivat yksinkertaiseen kyselyyn, jossa heidän

tuli ilmaista valmiutensa luovuttaa henkilökohtaista tietoa itsestään eräälle pankille. Tiedon jakamista kannustettiin tässä vaiheessa 20 dollarin rahasummalla. Kokeen ensimmäisen ja toisen vaiheen välillä oli 12 viikon aikaväli, jotta koehenkilöt eivät kokeen toisessa vaiheessa muistaisi kokeen ensimmäistä vaihetta. Kokeen toisessa vaiheessa koehenkilöitä pyydettiin jakamaan henkilökohtaista tietoa itsestään eräälle pankille. Jakamista ei tällä kertaa kannustettu erillisellä rahallisella kannustimella. Verratessa ensimmäisen vaiheen ilmaistua valmiutta jakaa henkilökohtaista tietoa itsestä toisen vaiheen tosiasialliseen jaettuun tietoon, sai tutkimuksen ensimmäinen hypoteesi vahvaa tukea; koehenkilöt olivat jakaneet itsestään enemmän tietoa kuin mitä olivat sanoneensa olevansa valmiita jakamaan. Tutkimuksen toisen kokeen ensimmäisessä vaiheessa koehenkilöt vastasivat kyselyyn, jossa selvitettiin kuinka monta henkilökohtaisen tiedon piiriin kuuluvaa asiaa kuudestatoista listatusta asiasta he olisivat valmiita jakamaan joko eräälle pankille tai lääkeyhtiölle 20 dollarin kannustamana. Koehenkilöt vastasivat myös kuinka luotettavaksi tai riskialttiiksi kokivat näiden tietojen luovuttamisen joko kyseiselle pankille tai lääkeyhtiölle. Kokeen vaiheiden välissä oli seitsemän viikon aikaväli, jotta kokeen ensimmäisen vaiheen muistaminen ei vaikuttaisi toisen vaiheen vastauksiin. Kokeen toisessa vaiheessa koehenkilöitä pyydettiin jakamaan henkilökohtaista tietoa itsestään vastaamalla kyselyyn. Tutkimuksen ensimmäinen hypoteesi sai toisenkin kokeen tuloksista tukea; koehenkilöt antoivat jälleen enemmän tietoa itsestään kuin mitä olivat aiemmin sanoneet olevansa valmiita antamaan. Riskien tiedostamisen ja koehenkilöiden ilmoittaman aikomuksen välillä oli myös tilastollisesti merkitsevä yhteys, mikä antoi tukea tutkimuksen toiselle hypoteesille; riskialttiiksi mielletyssä konteksissa koehenkilöt sanovat olevansa valmiita jakamaan vähemmän henkilökohtaista tietoa itsestään. Sen sijaan riskien tiedostaminen ei ollut tilastollisesti merkitsevästi yhteydessä jaetun tiedon määrään; riskialttiudella ei ollut vaikutusta siihen kuinka paljon henkilökohtaista tietoa koehenkilöt jakoivat. Tutkimuksen kolmas hypoteesi luottamuksen vaikutuksesta jaetun tiedon määrään ei saanut kokeessa tilastollisesti merkitseviä tuloksia (Norberg ja muut 2007).

Norbergin ja muiden (2007) tutkimuksen kokeiden tulosten perusteella voidaan nähdä kuinka haastavaan asemaan yksityisyysparadoksi asettaa ne IT-alan ammattilaiset joiden vastuulle jää käyttäjien yksityisyyden turvaaminen palveluita kehittäessä, sillä tarjolla oleva tieto käyttäjien ilmoittamista tarpeista ja havaituista toimintatavoista ovat ristiriidassa keskenään (Barth ja Jong 2017). Tyypillisimpänä syynä käyttäjien keskuudessa ilmenevälle yksityisyyden turvaamisen vähäiselle panostamiselle on se, että yksityisyyden turvaaminen muuten kuin tietoturvaohjelmistoilla koetaan usein liian vaivalloiseksi (Schaik ja muut 2017). Norberg ja muut (2007) tuovat esille tilanteen ongelmallisuutta myös seuraavasti: Mikäli kuluttajat eivät oma-aloitteisesti jaksa turvata

omaa yksityisyyttään, tuleeko jonkin toisen tahon turvata se käyttäjien puolesta, vähentäen täten yksilön taakkaa oman yksityisyytensä turvaamisessa?

Tutkimustiedon valossa voidaan sanoa käyttäjien jakavan tietoa itsestään verkossa melko vapaasti vaikka kokisivatkin teoriassa yksityisyysasiat tärkeiksi. Tietoa luovutetaan esimerkiksi jos sillä saadaan tarjouksia tuotteista tai ne mahdollistavat pääsyn johonkin palveluun. Täten yksityisyyden voisi nähdä ottaneen jonkinlaisen roolin vaihdon välineenä käyttäjien keskuudessa. Käyttäjät arvioivat kyllä tietojensa luovuttamisen hyötyjä ja haittoja, mutta päätöksentekoon vaikuttavat tekijät arvotetaan usein niin, että esimerkiksi ystävien näkemykset painottuvat vahvemmin päätöksenteossa kuin tieto palveluntarjoajan yksityisyyttä loukkaavasta toiminnasta. Älypuhelinten sovellusten käyttöönoton kontekstissa on myös havaittu, että tilannekohtaiset tekijät saattavat vaikuttaa mihin lopputulokseen käyttäjät lopulta päätyvät, vaikka käyttäjillä ilmenisikin teoreettista halua suojella yksityisyyttään. Nämä edellä mainitut tekijät voivat selittää kuinka käyttäjien keskuudessa ilmenevät näkemykset yksityisyyden suojelemisen merkityksestä eivät vastaakaan käyttäjien tosiasiallista toimintaa. On myös havaittu, että toisinaan käyttäjät kokevat suojelevansa yksityisyyttään esimerkiksi sosiaalisen median alustoilla rajoittamalla viestintäänsä niin, että välttävät julkisia julkaisuja suosien niiden sijaan yksityisviestejä. Samalla käyttäjät yrittävät olla myös tarkkoja sen suhteen kenelle antavat oikeuden nähdä mitä materiaalia jakavat. Tämä toiminta viittaa tosiasiassa joko välinpitämättömyyteen tai tietämättömyyteen mitä tulee kolmansien osapuolien toimesta suoritettuun tiedonkeruuseen, jota sosiaalisen median alustoilla tapahtuu. Käyttäjät siis antavat näin toimimalla palveluntarjoajille ajan myötä enemmän ja enemmän tietoa itsestään mahdollisesti luullen samalla suojelevansa yksityisyyttään (Barth ja Jong 2017).

Yksityisyysparadoksin ilmenemiseen ei ole tarjolla yksiselitteistä syytä, vaan ilmiön uskotaan olevan useiden eri tekijöiden summa (Barth ja Jong 2017). Barth ja Jong (2017) pyrkivät kirjallisuuskatsauksessaan selittämään yksityisyysparadoksia riskien ja hyötyjen laskelmoinnin avulla, yhdistäen tähän käyttäjien rationaalisia ja irrationaalisia päätöksentekotapoja. Päätöksentekotavat voidaan määritellä rationaalisiksi jos ne ovat esimerkiksi loogisia, syy-seuraus-suhteellisia, sääntöihin pohjautuvia ja hierarkkisia. Yksilön tulee myös päätyä näihin päätöksiin tietoisesti ja olla sekä tietoinen näistä prosesseista että hallita niitä. Irrationaalisia päätöksentekotapoja kuvaavat rationaalista päätöksentekoa haittaavat tekijät kuten aikarajoitukset, välittömän mielihyvän halajaminen ja optimismiharha. Käyttäjät eivät usein tiedosta näitä rationaalista päätöksentekoa haittaavia tekijöitä, jolloin he päätyvät virheellisesti tekemään päätöksiä joissa tiedostavat vain päätöksistä seuraavat hyödyt jättäen riskit huomioimatta. Vaikka tämä rationaalisten päätöksentekoprosessien ja sitä rajoittavien tekijöiden perusteella suoritettava päätöksenteko saattaa aluksi kuulostaa hyvältä selittäjältä yksityisyysparadoksin ilmenemiselle, ovat Barth ja Jong (2017) skeptisiä sen suhteen,

onko se ainoa pätevä selittäjä käyttäjillä havaituille ristiriidoille aikomusten ja päätöksenteon suhteen.

5 Pohdinta

Tutkielman käsittelemät näkökulmat yksityisyyden ja tietoturvan suhteen olivat tutkielman laajuuden takia rajatut ja täten joitain olennaisia näkökulmia jäi tutkielmasta pois. Esimerkiksi sukupuolen merkitys siinä miten yksityisyyttä arvostetaan jää käsittelemättä iän ja kulttuurin yhteydessä (Miltgen ja Peyrat-Guillard 2014). Myös esineiden internetin (Internet of things) vaikutukset yksityisyyteen lienevät kiistattomia, mutta niitäkään ei käsitelty. Älypuhelinten sovellukset voivat tallentaa käyttäjien sijaintitietoja ja urheilun ja liikunta-aktiviteettien parissa hyödynnetyt mittarit voivat ladata kerätyn datan suoraan verkon pilvipalveluihin. Keskustelua on käyty myös autoihin asennettavista seurantalaitteista joiden avulla autoilijoita laskutettaisiin julkisten teiden käytöstä ajokilometrien mukaan (Liikenne- ja viestintäministeriö 2013). Iän vaikutuksen tutkimisen yhteydessä tutkimuksessa käsiteltiin yliopisto-opiskelijoita, mutta on mahdollista että tämä ryhmä nuoria omaa koulutustaustaltaan erilaiset näkemykset kuin eri koulutustaustan omaavat nuoret. Kolmas keskustelua herättänyt, mutta tutkielmasta pois rajattu ilmiö, on terveydenhuollon piiriin liittyvä biopankkien toiminta. Biopankit keräävät näytteitä potilailta ja tallentavat ne myöhempää käyttöä varten, siinä missä tyypilliset tutkimusnäytekokoelmat eivät tallenna kerättyjä näytteitä, vaan ne hyödynnetään yksittäisissä tutkimuksissa jonka jälkeen näytteet poistetaan (Snell ja muut 2012). Tämänlainen terveystietoihin liittyvä henkilökohtaisen datan keruu ja tallettaminen voisi olla esimerkiksi Addaen ja muiden (2017) saamien tulosten valossa tärkeä asia yksityisyystietoisille henkilöille ja täten näkemykset biopankeista voisivat olla olennainen osa nyky-yhteiskunnan yksityisyyden luonteen tutkimusta.

Nuorten taitotaso ilmeni tutkielmassa yleisesti ottaen parempana kuin vanhempien ihmisten. Tätä taitotasoa ei tulkittu kuitenkaan kovin syvällisesti. Esimerkiksi evästeet raportoitiin Schaikin ja muiden (2017) tutkimuksessa pienimmäksi koettuna tietoturvauhkana. Evästeiden avulla sivustot voivat kuitenkin kerätä varsin paljon dataa käyttäjistä, eikä ole selvää johtuuko niihin liittyvien riskien kokeminen vähäisenä siitä, että käyttäjät eivät tiedosta täysin evästeisiin liittyviä tietoturvauhkia vai eikö näitä uhkia vain koeta merkittävinä suhteessa muihin verkon tietoturvauhkiin. On siis mahdollista, että vaikka nuoret ovat keskimäärin vanhempia ihmisiä parempia yksityisyytensä turvaamisessa verkossa, ei tämä osaaminen välttämättä ole syväluotaavaa. Täten myös IT-alan koulutuksen merkitys yksityisyyden turvaamisessa saattaisi olla hyvinkin relevantti tekijä, niin osaamisen kuin asenteiden osalta.

IT-alan ammattilaisten kehittelemään agenttipohjaiseen sovellukseen (Kökciyan ja muut 2017) liittyy luvussa 3 mainitun argumenttien painoarvojen huomiotta jättämisen

lisäksi muitakin ongelmia. Esimerkiksi verkon suoratoistopalveluiden kautta käyttäjät voivat jakaa videomateriaalia suoraan sosiaalisen median alustoilla. Tämä voi johtaa yhtälailla yksityisyyttä loukkaavan materiaalin jakoon ilman, että asianomaiset voisivat asiaan vaikuttaa, aivan kuten nykyinen tiedonjako ilman erillistä luvan pyytämistä. Agenttien toiminta vaikutti myös olevan riippuvaista siitä, että tietoa jakava käyttäjä merkitsee (tags) kaikki jaettavassa materiaalissa esiintyvät yksilöt. Ongelmallista tässä on kuitenkin se, että esimerkiksi jaettavassa kuvassa taustalla esiintyvä, mutta käyttäjälle tuntematon henkilö ei pääsisi vaikuttamaan kuvan julkaisemiseen koska käyttäjä ei luonnollisesti voi merkitä tälle tuntematonta henkilöä kuvassa esiintyväksi. Myös palveluun kuulumattomien yksilöiden yksityisyyttä ei voitaisi turvata, koska heillä ei olisi lainkaan agenttia käymässä keskusteluja heidän preferensseistään. Kenties asia olisi ratkaistavissa osittain esimerkiksi kuvien suhteen jonkinlaisella kasvojentunnistamissovelluksella joka vaatisi, että tietoa jakava käyttäjä merkitsisi kuvasta löydettyjä kasvoja vastaavien käyttäjien käyttäjänimet yrittäessään jakaa kyseisen kuvan.

6 Yhteenveto

Tutkielmassa käy ilmi, että yksityisyys ja sen turvaaminen on haastavassa asemassa tietoyhteiskunnassa. Yksityisyyden arvo tunnustetaan kyllä, mutta sen ylläpitäminen vaatii enemmän työtä kuin mitä moni on valmis tekemään. Yksityisyyden suojelemisen sijaan tyydytään luottamaan siihen, että tietoja keräävät tahot käyttävät tietoja kunnioittaen käyttäjien oikeuksien laiminlyönnistä johtavien sanktioiden pelossa. Kehitteillä olevat keinot parantaa käyttäjien tietoturvaa ja yksityisyydensuojaa sosiaalisessa mediassa ovat vielä toistaiseksi keskeneräisiä. Suuntana voisi olla siirtymä erillisestä kiellosta tiedon jakamiseen erilliseen lupaan jakaa tietoa, mutta tämä vaatisi sosiaalisen median alustoilta halua tehdä yhteistyötä ja muovautua näiden uusien vaatimusten mukaisiksi. Tämän lisäksi myös käyttäjien välisen yhteisymmärryksen saavuttaminen siinä minkälaisten sääntöjen mukaan vaikkapa sosiaalisen median alustoilla voi jakaa tietoa toisista käyttäjistä, on varmasti haastavaa. Kun huomioidaan vielä kulttuurin ja iän vaikutukset näkemyksiin yksityisyyden merkityksestä ja siitä mitä tietoa toisista sopii jakaa ja millä perustein, on helppoa huomata ettei yksinkertaista ratkaisua ongelmaan ole.

Viiteluettelo

Addae, J. H., Brown, M., Sun, X., Towey, D., M. and Radenkovic, M. (2017). Measuring attitude towards personal data for adaptive cybersecurity. Information and Computer Security. Vol. 25, Issue 5. 560-579. DOI:10.1108/ICS-11-2016-0085

Barth, S. and D.T. de Jong, M. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. Telematics and Informatics. Vol. 34, Issue 7. 1038-1058

Kökciyan, N., Yaglikci, N. and Yolum, P. (2017). An Argumentation Approach for Resolving Privacy Disputes in Online Social Networks. ACM Transactions on Internet Technology (TOIT). Vol. 17, Issue 3. Article No. 27

Kyberturvallisuuskeskus (2019). Tietoturva.
https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva
Haettu 29.11.2019

Liikenne- ja viestintäministeriö (2013). Ollilan työryhmä: Kokeiluin kohti kilometriverotusta. https://www.lvm.fi/-/ollilan-tyoryhma-kokeiluin-kohti-kilometriverotusta-789727 Haettu 8.12.2019

Martin K. E. (2012). Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract. Journal of Business Ethics. Vol. 111, Issue 4. 519–539

Miltgen, C. L. and Peyrat-guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. European Journal of Information Systems. Vol. 23, Issue 2. 103-125. DOI:10.1057/ejis.2013.17

Norberg, P. A., Horne, D. R. and Horne D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. The Journal of Consumer Affairs. Vol. 41, Issue 1. 100-126. DOI:10.1111/j.1745-6606.2006.00070.x

Presthus, W. and Sørum, H. (2018). Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation. Procedia Computer Science. Vol. 138. 603-611

Regan, P. M., FitzGerald, G. and Balint, P. (2013). Generational views of information privacy? Innovation: The European Journal of Social Sciences. Vol. 26, Issue 1/2: 81-99. DOI: 10.1080/13511610.2013.747650

Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J. and Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. Computers in Human Behavior. Vol. 75. 547-559

Snell, K., Starkbaum, J., Lauß, G., Vermeer, A and Helén, I. (2012). From Protection of Privacy to Control of Data Streams: A Focus Group Study on Biobanks in the Information Society. Public Health Genomics. Vol. 15, Issue 5. 293-302. DOI:10.1159/000336541

Tietosuojavaltuutetun toimisto (2019a). Tietosuoja turvaa oikeutesi henkilötietoja käsiteltäessä. https://tietosuoja.fi/tietosuoja Haettu 29.11.2019

Tietosuojavaltuutetun toimisto (2019b). Usein kysyttyä EU:n tietosuoja-asetuksesta. https://tietosuoja.fi/gdpr Tarkastettu 05.12.2019

Warren, S. and Brandeis, L. (1890). The Right to Privacy. Harward Law Review. Vol. 4, Issue 5. 193-220. DOI: 10.2307/1321160